Bob de Brabander ()

Filip Davidovic (1034603)

Lab on Offensive Computer Security – Assignment

Kaminsky DNS vulnerability

# Usage

## Example input

What follows is a template for input. It is to be given as input to a terminal or a command prompt

python kamins.py victimIP targetDomain yourDNSIP [-t/--ttl ttl] [-s/--silent -l/--loud]

Each of the given arguments is described below:

* victimIP – IP of the DNS server that is to be cache poisoned,
* targetDomain – domain (zone) that is to be spoofed. The domain should be **inputted without www in front of it**,
* yourDNSIP – IP of your DNS server (that is to be given as authoritative for the target domain). This argument can also be one of the following myip or myIP in order to put the user’s current public IP,
* ttl – time to live to be injected into the victim’s cache,
* -s – specifies the silent method for the attack,
* -l – specifies the loud method for the attack.
  + Note: only one of the above two can be used.